



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

May 24, 2007

FILED/ACCEPTED

MAY 24 2007

Federal Communications Commission
Office of the Secretary

Marlene H. Dortch, Secretary
Federal Communications Commission
c/o Natek, Inc.
236 Massachusetts Avenue, NE, Suite 110
Washington, D.C. 20002

Re: Appendices to Petition for Expedited Rulemaking Filed May 15, 2007

Dear Secretary Dortch:

On May 15, 2007, the United States Department of Justice filed a Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act. The petition referenced three appendices. Those appendices, however, were inadvertently omitted from the filing. This letter transmits the referenced appendices and requests that they be incorporated into the filing made on May 15.

An original and four copies of this letter and each of the three appendices are enclosed. Please date-stamp the extra copy and return it to the courier. Please contact the undersigned with any questions or concerns regarding this filing.

Respectfully submitted,

Original
11374

Elaine N. Lammert

Elaine N. Lammert
Deputy General Counsel
Federal Bureau of Investigation

Enclosures

cc: Tom Beers, PSHSB
Darryl Cooper, PSHSB

No. of Copies rec'd 016
List AECDE

APPENDIX A

TIA TR-45 Mobile and Personal Communications Systems Standards
 TR-45 Lawfully Authorized Electronic Surveillance Ad Hoc Group

TITLE: Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities
 for packet-based communications pursuant to the Communications Assistance for Law Enforcement
 Act (CALEA).

DATE: January 21, 2002

SOURCES:



CALEA Implementation Section
 Lou Degni
 14800 Conference Center Drive, Suite 300
 Chantilly, VA 20151-3810
 Tel: (703) 814-4729
 Fax: (703) 814-4720
 e-mail: ldegnil@askcalea.net

DISTRIBUTION: TR45 LAES Ad Hoc Group

ABSTRACT: This contribution proposes content for a Stage 1 description of capabilities needed
 by Law Enforcement Agencies for the surveillance of packet-based communications, pursuant to the
 Communications Assistance for Law Enforcement Act (CALEA). This material should provide a
 framework for refining the packet-based communications requirements published in J-STD-025,
 Lawfully Authorized Electronic Surveillance.

The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text or other
 copyrightable material contained in this contribution and any modifications thereof in the creation of a TIA Publication; to copyright and
 sell in TIA's name any TIA Publication even though it may include all or portions of this contribution; and at TIA's sole discretion to permit
 others to reproduce in whole or in part such contribution or the resulting TIA Publication. This contributor will also be willing to grant
 licenses under such copyrights to third parties on reasonable, non-discriminatory terms and conditions for purpose of practicing a TIA
 Publication which incorporates this contribution.

This document has been prepared by the contributors to assist the TIA Engineering Committee. It is proposed to the Committee as a basis
 for discussion and is not to be construed as a binding proposal on the contributors. The contributor specifically reserves the right to amend
 or modify the material contained herein and nothing herein shall be construed as conferring or offering licenses or rights with respect to any
 intellectual property of the contributors other than provided in the copyright statement above.

The company represented by this individual may have patents or published pending patent applications, the use of which may be essential
 to the practice of all or part of this contribution incorporated in a TIA Publication and the company represented by this individual is willing
 to grant a license to applicants for such intellectual property contained in this contribution in a manner consistent with 2a) or 2b) of Annex
 H of the TIA Engineering Manual.

Table of Contents

1		
2		
3	1. Introduction	4
4	1.1. Background and Context	4
5	1.2. Purpose and Scope of Contribution	5
6	1.3. Organization	5
7	1.4. Notation	5
8	2. Definitions	5
9	3. User Perspective of Law Enforcement Agency Needs (Stage 1)	8
10	3.1. Communications Access.....	8
11	3.1.1. Separate Access to Communication-Identifying Information and Communication	
12	Content	8
13	3.1.2. Access to Communication-Identifying Information	9
14	3.1.2.1. Subscriber Information	10
15	3.1.2.2. Network Protocol Identifiers and Service Access Ports	10
16	3.1.2.3. Signaling and Control Information	10
17	3.1.2.4. Communication Attempt Alerts	11
18	3.1.3. Access to Communication Content	12
19	3.1.4. Access Requirements for Specialized Service Capabilities	12
20	3.1.4.1. Forwarding, Redirected Communications, and Mobility	13
21	3.1.4.2. Multiple Recipients	13
22	3.1.5. Separation of Subscriber Physical Interface from the TC	13
23	3.1.6. Real-Time, Full-Time Access to Communications	14
24	3.1.7. Subject Verification and Subscriber Information	15
25	3.1.7.1. Association of Communications With Intercept Subject	15
26	3.1.7.2. Service Profile Information	16
27	3.2. Delivery of Intercepted Communications.....	16
28	3.2.1. Transmission	16
29	3.2.2. Correlation of Communication Content with Communication-Identifying Information	
30		17
31	3.2.3. Non-Alteration of Transmitted Content	17
32	3.2.4. Content Decoding, Decompression, and Decryption	17
33	3.2.5. Use of Standard, Generally Available Delivery Interface	18
34	3.2.6. Congruence With Existing Delivery Interfaces	18
35	3.2.7. Consolidated Delivery Interface and Transmission Facilities	19
36	3.3. Performance and Quality	19
37	3.3.1. Reliability	19
38	3.3.1.1. Availability	19
39	3.3.1.2. Fault Management	19
40	3.3.2. Quality of Service	20
41	3.3.3. Timing Requirements	20
42	3.3.3.1. Time Stamp Accuracy	20
43	3.3.3.2. Event Timing	20
44	3.4. Security and Integrity	21
45	3.4.1. Transparency of Interceptions	21
46	3.4.2. Security of Delivered Surveillance	21
47	3.4.2.1. Separation of Surveillance Interfaces from Subscriber Traffic	21
48	3.4.2.2. Encryption of Delivered Communication-Identifying Information and	
49	Communication Content	21
50	3.4.3. Procedural Safeguards	22

1	3.5.	Capacity and Transmission Bandwidth	22
2	3.5.1.	Simultaneous Interceptions	22
3	3.5.2.	Transmission Bandwi.....	23
4	4.	Recommendation.....	23
5			
6			

1. Introduction

1.1. Background and Context

Lawfully Authorized Electronic Surveillance (LAES) is a critically important investigative tool whereby law enforcement agencies are permitted to intercept communications and/or acquire “communication-identifying information”¹ of monitored subjects. Many serious criminal investigations would be thwarted without the availability of LAES as an investigative technique.

The legal authority for LAES is found in various federal statutes, including but not limited to the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3121 et seq., which governs the collection of called and calling party information through pen registers and trap and trace devices, and the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510, et seq., which governs interceptions of communications content and is commonly referred to as either “Title III” or the “Wiretap Act.” The assistance of Telecommunications Carriers (TCs)² in supporting LAES has long been authorized and required pursuant to these federal statutes. In addition, TCs are required to design their systems so as to ensure that they are capable of enabling the government to conduct LAES, pursuant to the 1994 Communications Assistance for Law Enforcement Act (CALEA).³ CALEA clarifies the extent to which a TC must provide capabilities to assist law enforcement in conducting LAES.

The current industry standard for the support of LAES is specified in TIA/EIA J-STD-025, *Lawfully Authorized Electronic Surveillance*. Although the focus of the J-STD-025 specification is the surveillance of predominantly circuit-mode communications (i.e., voice and data calls using circuit-switched transmission paths dedicated to each call), the specification includes requirements for the interception of packet-based communications. The Federal Communications Commission (FCC) issued a Third Report and Order upholding the packet-based portions of the J-STD-025 specification and requested further study of packet-based communications by the telecommunications industry.

The FCC held in the order released on September 21, 2001 that wireline, cellular, and broadband PCS carriers must implement a packet-based communications surveillance capability by November 19, 2001.

The advent and advances in the use of packet-based switching and transport technologies for the conveyance of communications has challenged the ability of service providers to support LAES functionality. Increasingly, many new packet-based communications services and architectures have been developed which impede or even preclude the use of LAES. Such packet-based communications services may include, but are not necessarily limited to Public IP Network Access and Transport services, Carrier-Grade Voice-Over-Packet (CGVoP) services, Voice over Packet

¹ The term “communication-identifying information” is defined in this document as dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by the subscriber by means of any equipment, facility, or service of a TC. The term is intended to be understood as covering the same information described in the Communications Assistance for Law Enforcement Act, 41 U.S.C. 1001(2) as “call identifying information.”

² The terms Telecommunications Carriers (TCs) and carriers are used synonymously and interchangeably in this contribution.

³ See generally 47 U.S.C. §1001 to §1010; CALEA applies to telecommunications carriers but not to information services. See 47 U.S.C. §§1002(b)(2)(A), 1001(6).

Internet Gateway (VPIGW) services, and Wireless IP services. These packet-based communications services can be provided via either landline (e.g., dial-up analog, Digital Subscriber Line (xDSL), or cable modem) or wireless access technologies.

The J-STD-025 specification addresses LAES for packet-based communications only at a high-level and does so primarily by providing for the delivery of the entire packet stream associated with an intercept subject. In particular, the packet-based communications surveillance capabilities in the J-STD-025 specification do not explicitly identify the communication-identifying information-aspects of the packet-mode surveillance solution, nor does it address aspects of packet-based communications content delivery, which differ from the current circuit-mode content delivery capabilities. In order to guide TCs in further revising LAES solutions for the surveillance of packet-based communications, extensions to the J-STD-025 specification are needed. The first stage in defining such extensions is the definition of end-user (i.e., law enforcement) needs for LAES capabilities in the TC networks that support packet-based communications services.

1.2. Purpose and Scope of Contribution

The purpose of this contribution is to define the capabilities needed, from a Law Enforcement Agency (LEA) perspective, to support LAES of packet-based communications and the interface between TCs and the surveillance collection systems of LEAs. Specifically, it provides a “Stage 1” user-view description of the general capabilities, features, and information needed by law enforcement for LAES of packet-based communications.

1.3. Organization

The remainder of this contribution is organized as follows:

- Section 2 summarizes key terms and acronyms used in this contribution, and where necessary, expands the definitions contained in 3-STD-025 for the circuit-mode environment to accommodate the packet-mode environment as well.
- Section 3 describes the approach law enforcement has taken towards LAES of packet-based communications.
- Section 4 defines the fundamental needs of law enforcement for LAES in a packet-mode environment.
- Section 5 proposes how this Stage 1 description would be incorporated into J-STD-025.

1.4. Notation

In this document, Law Enforcement needs are identified in terms of essential capabilities, tagged with the notation (EC), and sequentially numbered.

2. Definitions

Associate (expanded J-STD-025 definition⁴)

A telecommunication user whose equipment, facilities, or services are used to communicate or attempt to communicate with a subject.

Intercept Subject or Subject (expanded J-STD-025 definition⁵)

A telecommunication service subscriber whose incoming, outgoing, and redirected c'ommunications, call- or communication-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

Communication (same as J-STD-025 definition)

Communications encompasses the term “electronic communications,” as defined in 18, U.S.C. 2510(12), any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system, etc. As used herein, the term also includes the term “wire communications” as defined in 18, U.S.C. 2510(1).

Communication-Identifying Information (same as J-STD-025 definition as Call-Identifying Information)

Communication-identifying information, as used in this document, is synonymous with call-identifying information. As defined in CALEA, the “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a TC. (47 U.S.C. Section 1001(2)).”⁶

Communications Content (correction of J-STD-025 definition for Content)

Defined in 18 U.S.C. 2510 (8) to be “when used with respect to any wire, oral or electronic communications, includes any information concerning the substance, purport, or meaning of that communication.”

Communications Session (or Session) (new definition)

The duration between establishment and release of the capability for the transmission of communication between an intercept subject and the service provider’s network, during which communication may occur between the subject and one or more associates.

Communication attempt (new definition)

⁴ The J-STD-025 definition for Associate is “a telecommunication user whose equipment, facilities, or services are communicating with a subject.”

⁵ The J-STD-025 definition for Intercept subject is “a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).”

⁶ See also Section 3.1.2 for examples of communication-identifying information for packet-based services as addressed in this document.

1
2 The initiation (successful or unsuccessful) of communication between the intercept subject and an
3 associate by either party.
4

5 **Session Identifier (new definition)**

6
7 Unique identifier for the intercept subject's network access session in a service provider's network. If
8 content surveillance is authorized, this parameter uniquely identifies the network access session for
9 which the subject's incoming, outgoing, and redirected packet activity is to be delivered to a LEA,
10 and is used to correlate communication-identifying information with the communication content.
11

12 **Minimization (new definition)**

13
14 A procedure that law enforcement officers are required to apply when conducting **LAES** so as to
15 minimize the interception of communications not otherwise subject to interception. See 18 U.S.C. §
16 2518(5).
17
18

3. User Perspective of Law Enforcement Agency Needs (Stage I)

The essential capabilities provided in this contribution are based on law enforcement needs regarding surveillance of packet-based communications. Many of these capabilities are similar to existing capabilities for circuit-mode communications, but are generalized to include packet-based communications. Others prescribe additional functionality specific to the surveillance of packet-based communications services.

The capabilities are grouped into the following functional categories as addressed in the corresponding sections of this contribution:

- Communications Access (3.1)
- Delivery of Intercepted Communications (3.2)
- Performance and Quality (3.3)
- Security and Integrity (3.4)
- Capacity (3.5).

3.1. Communications Access

3.1.1. Separate Access to Communication-Identifying Information and Communication Content

(EC) 1. Law enforcement agencies need separate access to an intercept subject's communication-identifying information and communication content (when access to communication content is authorized), consistent with the scope of lawful authorization.

The terms communication-identifying information and communication content are used to describe specific aspects of packet-based communications surveillance and are described below in more detail in an effort to clarify their use in the packet-mode context. The use of the communication-identifying information and communication content terms is intended to be understood as covering the same information described in the Communications Assistance for Law Enforcement Act, 47 U.S.C. 1001(2) as "call identifying information" and "content".

- Communication-identifying information for packet-based communications refers to the information necessary to identify the intercept subject's communications traffic, to determine the parties to a packet-based communication, and to describe, qualify, or otherwise determine, the origin, direction, destination, or termination of the intercept subject's communications.
- Communication content for packet-based communications refers to information concerning the substance, purport or meaning of the communications contained within the intercept subject's incoming, outgoing, or redirected packet data.

In the packet environment, communications content may include both voice and data communications of the intercept subject as transported by the packet-based equipment for the purpose of providing a service.

The specific nature of the communication-identifying information in the packet environment may vary according to the nature of the communications service provided and the mechanisms and

protocols used to carry the communications to and from the intercept subject and the associates. Associates may include other end-users, equipment, facilities, services, or entities that communicate with or attempt to communicate with the intercept subject via the subject's service. Examples may include other subscribers to the service, subscribers of other, interconnected TCs, or entities otherwise accessible to the intercept subject via the service.

More specific capabilities for law enforcement access to communication-identifying information and communications content in the packet environment are discussed in Sections 3.1.2 and 3.1.3, respectively.

3.1.2. Access to Communication-Identifying Information

(EC) 2. Law enforcement agencies need access to available communication-identifying information to determine the parties to a communication (originating and terminating), or otherwise determine the origin, direction, destination, or termination of the intercept subject's communications, regardless of whether or not interception of communication content is authorized.

(EC) 3. Law enforcement agencies need access to communication-identifying information for all completed and attempted communications. An attempted communication is one that was initiated, but fails to complete between the originating (source) and terminating (destination) parties (e.g., a failed voice call due to unavailable terminating party equipment, or data packets originated by the subject that could not be delivered to an associate).

(EC) 4. Law enforcement agencies need any success or failure information available to the carrier regarding each communication.

Law enforcement recognizes that there may be instances where certain information for attempted communications may not be available.

Communication-identifying information for packet-based communications may include, but is not necessarily limited to, information in the following categories:

- Subscriber Information - Information regarding the intercept subject's and associates' subscriber identification and service. This may include network addresses (e.g., Directory Numbers (DNs), Internet Protocol (IP) addresses), service account identifiers, and subscriber service information.
- Network Protocol Identifiers and Service Access Ports of Subject Traffic - The network protocol identifiers, and transport-layer service access port numbers of packets generated by or destined to the intercept subject, regardless of whether the communications is successfully delivered to the intended destination.
- Signaling and Control Information - Information used in communication establishment, maintenance and termination, as relevant to the service. This should include redirection or re-routing indications, when available.
- Communication Attempt Alerts - Notification that a communication attempt concerning the intercept subject has occurred.

3.1.2.1. *Subscriber Information*

(EC) 5. Law enforcement agencies need access to available Subscriber Information associated with each communication generated by or destined to the intercept subject. Subscriber Information⁷ includes, but is not necessarily limited to, the following information about the intercept subject and the associates with whom the subject communicates:

1. Network Addresses – Information used by the network for sending and receiving communications to and from the intercept subject. This may include addresses provided to and by network address translation mechanisms. The intercept subject's and associates' network addresses may include, but are not necessarily limited to, Directory Numbers (DNs), mobile station identifiers, Internet Protocol (IP) addresses (dynamically assigned or static), and domain names.
2. Service Account Identifiers* – Information provided by a subscriber to the TC for access to network resources and identification of the allowed services. A subscriber's service account identifiers may include, but are not necessarily limited to, login identifiers (IDs), account numbers, and subaccount numbers. Because subscribers' network address information may be associated with a subscriber for only a limited period of time, such as the duration of a network access communications session, in many cases, a Service Account Identifier is the only information that is permanent and available to the carrier (and law enforcement) for identification of the subscriber and his/her traffic.
3. Subscriber Service Information – Additional characteristics about the nature of the communication that identify the capabilities of the service as used by the intercept subject (e.g., authorized bandwidth for the subscriber's communications session or call, encoding format of communications). Access to this information for the intercept's associates may be limited to what is received by the TC during the communication establishment stage.

3.1.2.2. *Network Protocol Identifiers and Service Access Ports*

(EC) 6. Law enforcement agencies need access to the network protocol identifiers (i.e., the IP header field that identifies the Transport Layer protocol) and transport-layer service access ports used in a communication in order to identify the network-relevant services that the subject is using and/or providing.

Such information may be provided, for example, in the transport-layer protocol (e.g., TCP or UDP) headers of data packets associated with the intercept subject.

3.1.2.3. *Signaling and Control Information*

⁷Information regarding the intercept subject's subscriber identification. In packet networks it is often the case that the facilities used to identify the intercept subject's communications are logical rather than physical and fixed. Subscriber Identification Information is the term used in this document for the identification of the intercept subject's "logical facilities" associated with the service offered by the carrier.

⁸ Service account identifier information can be provided to the carrier by passive means (e.g., intercept subject equipment provides this information to the network) or actively input by the intercept subject (e.g., submission of a login ID to the TC).

(EC) 7. Law enforcement agencies need access to reasonably available signaling and control information for all Communications originated by, terminated to, or redirected by the intercept subject for the service under LAES. This information is needed regardless of whether it is carried in-band with content or on out-of-band signaling channels (either physically or logically separated). Signaling and control information includes, but is not necessarily limited to, the following:

1. Account login events that indicate when an intercept subject has initiated a communications service or network access communications session with the service provider's network (e.g., access to the resources associated with the VPIGW service).
2. All communication-identifying digits dialed by the subject, or otherwise input (e.g., E.164 addresses and abbreviated dialing sequences) and any signaling information used to establish or direct call flow or activate service features (e.g., such as three-way calling for a CGVoP service).
3. Routing information derived by the originating TC based on its interpretation of the subject's user input or other call direction commands.
4. Redirecting routing information, when communications are forwarded or transferred using service capabilities. Law enforcement needs access to the redirected-to routing information when the intercept subject transfers or forwards communications to another address. For a communication terminating to the intercept subject, law enforcement agencies need access to any available redirection address information when multiple forwards or transfers are involved in the communication attempt⁹.
5. Location of mobile subscribers. Law enforcement agencies need information on the most accurate geographical information known to the network about the location of a mobile subscriber at the establishment and termination of each intercepted packet-based call or communications session, where such location information is relevant to the control of the call or communication session within and between carrier networks.
6. Changes initiated by the intercept subject (sent to the TC's network) to the encoding characteristics of the content stream (e.g., dynamic CODEC changes to a VoP communications stream).

3.1.2.4. Communication Attempt Alerts

(EC) 8. Law enforcement agencies need notification of all communication attempts generated by or destined to the intercept subject, when known by the TC for that service, regardless of whether or not those communications attempts are successful.

Such communications attempts include, but are not necessarily limited to:

1. Attempts to establish a network access communications session (e.g., successful or failed logins or mobile binding establishment attempts).
2. Successful and unsuccessful communications attempts generated by or destined to the intercept subject.

⁹ Redirected-to routing information is required for multiple forwards or transfers as long as the subject's equipment, facility, or service continues to be involved in the communication.

3. Data packet activity between an intercept subject and an associate, including successfully transferred packets and denied, blocked or rejected packets.

3.1.3. Access to Communication Content

LEA access to communication content for packet-based communications services is needed regardless of the service architecture used in the communication, including cases when the communications between the intercept subject and associates are sent and received over separate channels, or may be accessed at different IAPs at different geographical locations in the carrier's network.

(EC) 9. Law enforcement agencies need access to the communications transmitted, or caused to be transmitted, to and from the network address, terminal equipment, or other identifier associated with the intercept subject throughout the service areas operated by the TC served with the lawful authorization.

The communications between the intercept subject and other parties (associates) may take place using a variety of access and packet transport technologies, including cable, digital subscriber line (xDSL), IP, frame relay, and asynchronous transfer mode. In many cases these technologies may be combined in a carrier's network with numerous potential intercept access points for the intercept subject's communications content.

There are several ways to establish and maintain subscriber connections in a packet environment. Connection arrangements may be categorized as follows:

- Carriers may offer their services using connection-oriented technology and protocols where a dedicated path or virtual path is established through the network prior to a communication exchange.
- Carriers may offer their service utilizing connectionless technology and protocols where each packet in a communication is routed individually.

The specific nature of the accessed communications content may vary according to the service and the technology employed. Communication content includes any type of information carried by the carrier to or from the intercept subject (that is, any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature). For voice services, such as CGVoP or VPIGW, accessed content shall consist of the transported packets containing the encoded voice communications along with sufficient protocol information to decode and decrypt the voice-hand contents. For non-voice services, content refers to the transported application data payloads comprising the intercept subject's communications.

3.1.4. Access Requirements for Specialized Service Capabilities

Access to an intercept subject's packet-based communications shall include communications that involve the use of specialized service capabilities such as packet forwarding, mobility information, network-based encryption, and multi-way communications.

3.1.4.1. *Forwarding, Redirected Communications, and Mobility*

(EC) 10. Law enforcement agencies need access to communication content for communications generated by and destined to the intercept subject, including communications that have been redirected or have multiple communication recipients.

(EC) 11. For redirected (forwarded or transferred) communications, law enforcement agencies need access to the intercept subject's communications until the carrier's network no longer has access to the communication.

(EC) 12. If access to an intercept subject's communications cannot be maintained, law enforcement agencies need carriers to provide, as part of communication-identifying information, the identity of the new carrier and/or service area to law enforcement. The identity of the new TC and/or service area should be provided to law enforcement as soon as it is available.

(EC) 13. If the new TC's¹⁰ or service area's identity is unavailable, law enforcement agencies need to be provided with any information that will permit the LEA to determine or infer this information.

3.1.4.2. *Multiple Recipients*

(EC) 14. Law enforcement agencies need continuous access to communication content for services involving multiple communication recipients (for example, voice communications involving conference calls to multiple associates).

(EC) 15. Law enforcement agencies need access to communication content when the intercept subject's communication stream is placed on hold during a multi-way communication, but the remaining parties' communications continue to be supported by the intercept subject's equipment, facilities, or service. Law enforcement needs continued access to the remaining parties' communications as long as the carrier maintains access to the communication.

Law enforcement must be able to determine when to continue monitoring a communication and when to minimize the monitoring activity based on the circumstances of the investigation. (See the definition for minimization in Section 2.) In this case, law enforcement will arrange for any additional bandwidth necessary for the delivery of intercepted information.

3.1.5. *Separation of Subscriber Physical Interface from the TC*

Packet technologies allow for the separation of a subscriber's physical interface to the packet network from the carrier that provides the communications service to the subscriber. In these cases, different carrier(s) may provide the connectivity between the intercept subject and the carrier network that is offering a packet-based service and must facilitate LAES for the service. This case is similar to a scenario in the circuit-switched wireline environment where an Incumbent Local Exchange Carrier (ILEC) provides the distribution facilities to the intercept subject, but a

¹⁰ Note that the new TC may not be geographically located in the same area as the TC serving the intercept subject.

Competitive Local Exchange Carrier provides the voice service (via its PSTN switch). In this scenario, the CLEC is the service provider that may provide the **LAES** assistance capabilities”

(EC)17. In cases where an intercept subject’s physical interface to the *packet network* is separated from the carrier that provides the packet-based communications service for which the intercept subject is under **LAES**, the ability to facilitate lawful access to communication content and communication-identifying information is with the TC that offers the packet-based communications service to the intercept subject, and has access to communication-identifying information and communications content for the subject. This applies even if that TC does not necessarily offer direct physical connectivity (via their own facilities) to the intercept subject.

Law enforcement recognizes a carrier’s access to the **LAES** information may be constrained. Specifically, the carrier may have access to only the communication-identifying information and partial access or even no access to the communication content, as it may bypass the carrier providing the service and assistance to law enforcement. While the content for the communications may bypass the carrier providing the service, the carrier providing the service is the only carrier that may have knowledge of the establishment of the call or communications session and the identities of the communication endpoints for that call or communications session (via the service account identifiers and routing information for the two end points).

(EC)18. In the case where the TC’s access to the intercept subject’s communications are constrained, law enforcement agencies need access to all communications content and communication-identifying information of the intercept subject available to the carrier, and any additional information that would assist law enforcement in determining the service area or other carrier(s) that have access to any additional information or communications of the subject that are authorized to be intercepted.

This handoff information will enable law enforcement agencies to determine other service area(s) and/or carrier(s) from which surveillance is needed.

3.1.6. Real-Time, Full-Time Access to Communications

(EC) 19. Law enforcement agencies need a real-time monitoring capability for interceptions of packet-based communications. The term “real-time” refers to the ability to access and monitor communications that occurs concurrently with the transmission to or from the intercept subject’s equipment, facility, or service.

In actuality, there is a small transmission or propagation delay from the moment the intercept subject’s communications are intercepted until the moment the signals reach the **LEA** monitoring equipment. The immediacy with which the carrier must provide access to the intercept subject’s communications will vary according to aspects of the communications being accessed:

- For communication-identifying information, this will depend upon the nature of the communication-identifying information:

¹¹ In this scenario, the **LAES** assistance responsibilities are performed by the competitive local exchange carrier who provides the switch-based voice service to the intercept subject.

- 1 - For communication-management-related communication-identifying
2 information (i.e., the information used to identify, direct and control the intercept
3 subject's traffic), real-time refers to access that occurs concurrently with the
4 establishment and control of a *call* or communications session. Access to
5 communication-identifying information generated during call or communications
6 session establishment shall be provided before, during or immediately after the
7 transmission to or from the intercept subject.
8
- 9 - For **non-connection-management** associated events (for example, service profile
10 changes, or changes to the intercept subject's subscriber account information), real-
11 time refers to access that occurs **as** soon as the information **is** available to the carrier
12 and can reasonably be made available to law enforcement. (See also Section 3.1.7.2
13 regarding the reporting of service profile changes.)
14
- 15 • For communications content, real-time refers to intercept and delivery that occurs
16 concurrently with the transmission of communications to or from the intercept subject (in
17 other words, as the communications takes place).
18

19 Additional needs related to the immediacy of delivery of communication-identifying information and
20 communications content to law enforcement on the delivery interface are addressed in Section 3.1.7.
21

22 **(EC) 20.** Law enforcement agencies require a full-time monitoring capability for interceptions
23 of packet-based communications. The term "full-time" refers to the ability to access and monitor
24 all service activity associated with the intercept subject on a 24 hour-per-day basis.
25

26 **3.1.7. Subject Verification and Subscriber Information**

27
28 Law enforcement agencies need administrative information from the TC for non-connection
29 management associated events to verify the association of the intercepted packet-based
30 communications with the intercept subject, and to identify the services and features subscribed to by
31 the intercept subject, both prior to intercept implementation and during the interception.
32

33 **3.1.7.1. Association of Communications With *Intercept* Subject**

34
35 **(EC) 21.** Law enforcement agencies need, both prior to intercept implementation and during the
36 interception, information necessary to verify the association of the intercepted communications
37 with the network identifier (e.g., DN, login ID, IP address), terminal equipment identifier (e.g.,
38 MAC Address), and/or personal number of the intercept subject designated in the lawful
39 authorization. Specifically, law enforcement agencies must be able to verify that the
40 communications facility or service being intercepted corresponds to the subject or subjects
41 identified in the lawful authorization.
42

43 TCs are not expected to verify the type of communications (i.e., the application of the content
44 channel) used by the intercept subject beyond the service offered by the carrier.
45

46 **3.1.7.1.1. Association of Dynamic Addresses and Service Account Identifiers**

41

In many packet-based communications services, the addressing used to route the intercept subject's communications (e.g., an IP address) is dynamically assigned upon the establishment of a communications session and is released upon termination of the communications session, such that it must be correlated with a permanent subscriber identifier for the service (e.g., a directory number, login ID, or account number of the intercept subject).

(EC) 22. During interception of packet-based communications services where the address used to identify and route an intercept subject's communications is dynamically assigned, law enforcement agencies need the TC to provide the following information as part of communication-identifying information for the intercepted communications:

1. the temporary address dynamically assigned to the intercept subject and used for the communications session;
2. the key identifier(s) used by the carrier to associate the intercept subject's identity with the dynamically assigned address;
3. a unique identifier for the communication session; and
4. a time-stamp, which is necessary to correlate the dynamic address with the intercept subject's identity for the duration of the communications session.

3.1.7.2. Service Profile Information

Law enforcement agencies need the intercept subject's service profile information (subscription information) in response to a lawful inquiry. Service profile information may be required before and during interception.

(EC) 23. Law enforcement agencies need notification from carriers of changes made to the intercept subject's service profile during an ongoing interception when changes are directly initiated by the intercept subject.

Service profile information is needed to determine service features and capabilities the intercept subject might use and, correspondingly, how much capacity should be allocated to perform the LAES. For example, the subject of an ongoing interception may add additional bandwidth to their service. In this case, law enforcement may use the service profile change information to determine whether to update the intercept authorization and/or arrange for additional bandwidth to support the delivery of intercepted communications.

3.2. Delivery of Intercepted Communications

3.2.1. Transmission

(EC) 24. Law enforcement agencies need TCs to transmit intercepted communications to an LEA monitoring facility designated by the law enforcement agency.

Law enforcement agencies will work with TCs in advance to arrange for delivery of intercepted communications to the LEA's monitoring location. Guidelines for the transmission of intercepted communications are included in Sections 3.2.2 through 3.2.7.

3.2.2. Correlation of Communication Content with Communication-Identifying Information

(EC) 25. If communication-identifying information and communication content are separated, law enforcement agencies need TCs to provide identifiers on the delivery interface that will ensure accurate association of the communication-identifying information with communication content.

For certain packet-based communications where communication content surveillance is authorized, it should include appropriate encapsulation of the subject's sent and received packets within delivery messages appropriate for the delivery interface. Those delivery interface messages must contain added correlation descriptors that can be used to associate each packet with the intercept subject's service, and a specific packet-based communications session or call reported via communication-identifying information.

3.2.3. Non-Alteration of Transmitted Content

(EC) 26. Law enforcement agencies need TCs to be able to transmit the intercepted communications to an LEA monitoring location without altering the communication content or meaning (exclusive of any processing [e.g., protocol/encoding format changes, encryption] required for delivery to law enforcement).

(EC) 27. Law enforcement agencies need TCs to protect intercept controls, intercepted call content, and communication-identifying information consistent with the carrier's security policies and procedures in order to prevent unauthorized access, alteration, mutilation or manipulation, and disclosure of the transported data.

Any minimization of the intercept subject's communication content (*see* definition in Section 2) in order to comply with the lawful intercept authorization is the sole responsibility of the law enforcement agency.

3.2.4. Content Decoding, Decompression, and Decryption

Law enforcement agencies' collection systems must be able to properly process communication content delivered by the TC. Intercept subject communications are encoded, and could also be compressed and encrypted.

If the TC provides or controls the encoding, compression and/or encryption for the intercept subject's communications or at least is knowledgeable of this processing, the TC must either transmit the communication content in a decoded, decompressed and decrypted form, or provide the information (e.g., encoding method, compression method, encryption keys) needed by the law enforcement agency's collection system to perform this processing.

(EC) 28. When the TC provides or controls the encoding, compression and/or encryption for the intercept subject's communications or at least is knowledgeable of this processing, law enforcement needs the TC to either transmit the communication content, when authorized, toward the law enforcement agency's collection system in a decoded, decompressed and decrypted form, or provide to the law enforcement agency's collection system the information necessary to decode, decompress and/or decrypt the communication content.

Law enforcement prefers that the TC perform any decoding, decompression and/or decryption prior to the delivery of communication content. Since some of the communication content may be sent using proprietary protocols or special encoding formats that may make it difficult for law enforcement to convert back to the original end user communication, this preference is greater if proprietary or specialized encoding, compression and/or encryption had been used.

For cases where carriers provide network-based encryption, protocol conversion, or special encoding for intercept subject traffic, it is desirable for the carrier to provide access to communication content prior to encryption, conversion and/or encoding for traffic that is ingressive to the network and after encryption, conversion and/or encoding for egress traffic.

When pre- or post-encryption/conversion/encoding access is not provided for such specially modified traffic, carriers should provide all information available to the network that would facilitate law enforcement's ability to analyze, decode, decrypt, and/or convert the content stream, understand the involved protocols or encoding formats, or otherwise discern the content.

For example, if an intercept subject uses a voice service over a packet network where the subject's equipment encodes the communications stream based on a command from the carrier, when delivering this communication content to law enforcement, the carrier should provide information on the encoding scheme used for the communication in addition to delivering the content itself.

Similarly, if the carrier's network provides secure virtual private networking services for the subject or associates, including network tunneling with encryption, the carrier is expected to provide either the decrypted content stream or information on the protocols and encryption keys used to encrypt the content.

3.2.5. Use of Standard, Generally Available Delivery Interface

It is highly desirable to law enforcement agencies that the facilities, data communications protocols, and data format used for the transmission of the intercepted communications to the LEA monitoring location be standard, cost effective, and generally available.

Examples of such common, generally available, delivery interface technologies include Digital Signal/Level 0 (DS0) facilities, ATM Permanent Virtual Circuits (PVCs), IP Version 4 (IPv4) packets at the network layer, and the Transmission Control Protocol (TCP) at the transport layer. Additional protocols and formats can be jointly agreed upon by law enforcement and TCs.

3.2.6. Congruence With Existing Delivery Interfaces

Law enforcement recognizes that the CALEA law does not limit the number or types of interfaces used for the transmission of the intercepted communications to an LEA monitoring location.

However, it is highly desirable to law enforcement that TCs reuse or apply formatting from existing specifications for surveillance delivery interfaces for their service. The intention is to consolidate the number of interfaces law enforcement will need to comply with. For example, when developing a surveillance delivery interface for voice services over a packet network, an implementation's adoption of traditional J-STD-025 messages and parameters (where applicable) would be highly desirable for law enforcement.

It is highly desirable to law enforcement that TCs reuse or re-apply message formatting and encoding definitions from existing specifications, including the J-STD-025 specification, for the surveillance delivery interfaces for comparable packet-based communication services.

3.2.7. Consolidated Delivery Interface and Transmission Facilities

It is highly desirable to law enforcement that TCs minimize the number of physical transmission facilities used to deliver the intercepted communications to each LEA monitoring facility.

For example, in many Voice over Packet solutions several network elements may be involved in the interception of communication content and communication-identifying information. In these cases, law enforcement would prefer a connection from a single centralized delivery function or system to the monitoring facility, rather than several connections from each network element involved in the surveillance access.

3.3. Performance and Quality

3.3.1. Reliability

Reliability refers to the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions.

3.3.1.1. Availability

Some packet-based communications services may be offered with specific levels of reliability to subscribers as part of its service-level agreements. Other packet-based communications services are offered with grades of reliability, such that there are no assurances provided for establishing a transport-layer connection to the destination point or the successful delivery of subscriber messages to their intended destinations. In these cases, the network does not make any assurances on the quality or reliability of the communication service offered to the subscriber.

(EC)29. During the interception period, law enforcement agencies need the reliability of the service supporting the interception be at least equal to the reliability of the subject's service, when the network assures the reliability of the communication service offered to the subscriber.

(EC)30. During the interception period, law enforcement agencies need the reliability of the service supporting the interception be higher than the reliability of the intercept subject's service, when the network does not make any assurances on the reliability of the communication service offered to the subscriber.

(EC) 31. Law enforcement agencies require reliable delivery to the LEA collection system regardless of whether reliable delivery methods are employed by the network in offering service to the intercept subject.

(EC) 32. Law enforcement needs TCs to establish plans for ensuring that system upgrades, software upgrades, and other network management procedures do not disrupt or terminate ongoing interceptions.

3.3.1.2. Fault Management

(EC) 33. Law enforcement agencies need carriers to support capabilities to detect and resolve problems with

1. the interception of communication-identifying information and communication content; and
2. the transmission of the intercepted communications to the designated LEA monitoring facility.

3.3.2. Quality of Service

Quality of service in regard to the interception refers to the quality specification of the communications channel or system used to transmit the intercepted communications to the LEA monitoring facility. For example, quality of service may be measured based on quantitative factors, such as packet loss, bit error rate, or any other parameter used to measure transmission quality.

(EC) 34. Law enforcement agencies need for the quality of service of the intercepted transmissions delivered to the LEA monitoring facility to comply with performance standards of TCs for the monitored packet-based communications service.

3.3.3. Timing Requirements

Accurate time-stamps and prompt delivery of intercepted packet-based communications to the monitoring facility are critical to the conduct of law enforcement investigations. The following capabilities address these aspects of LAES.

3.3.3.1. Time Stamp Accuracy

Law enforcement agencies need time stamp information to correlate the communication-identifying information with delivered communications content.

Communication-identifying message must be time stamped within a specific amount of time from when the event triggering the message occurred. This time stamp would allow the LEA to associate the message with the communication content.

(EC) 35. Law enforcement agencies need communication-identifying information to be time-stamped within a specific amount of time from when an event triggering the generation of the communication-identifying information occurs. Time stamping shall be provided for encapsulated intercept subject packets delivered to the LEA.

3.3.3.2. Event Timing

Communication-identifying information must be transmitted over the delivery interface to the LEA collection system within a defined amount of time after the event occurs, in order for the LEA to correctly associate the communication-identifying information with communication content.

(EC) 36. Law enforcement agencies need communication-identifying information within a defined amount of time after the occurrence of the corresponding event in the network.

3.4. *Security and Integrity*

3.4.1. *Transparency of Interceptions*

(EC) 37. Law enforcement agencies need each interception to be transparent to the subject, the subject's associates, and to all parties except the investigative agency or agencies requesting the interception, and specific individuals involved in implementing the intercept capability. At a minimum, the transparency of an interception must satisfy the following criteria:

1. Indications that an interception is underway should not be discernible to anyone using the subject facilities or other any other parties.
2. If the implementation of an interception occurs during an ongoing communication, the interception should not disrupt or interrupt the ongoing communication (that is, no interruption or alteration of communications shall occur on active channels).
3. If the implementation of an interception causes changes in the operation of services and features, such changes should not be perceptible to the subject or other parties.
4. If any noise/packet loss/increased latency/error rate increase is introduced by the implementation of an interception, such noise/packet loss/increased latency/error rate increase should not be perceptible to the subject or other parties.

Law enforcement agencies need TCs to notify the appropriate law enforcement agency upon learning that intercept transparency was or may have been compromised. In such a situation, TCs should recognize that time is of the essence because the safety of the public and other law enforcement officers may be at risk.

To meet law enforcement needs for transparency, the services and transmission characteristics provided to the intercept subject or any other subscriber should continue to comply with industry standards.

3.4.2. *Security of Delivered Surveillance*

3.4.2.1. *Separation of Surveillance Interfaces from Subscriber Traffic*

(EC) 38. If any part of a surveillance solution employed by a carrier uses shared network resources with its subscribers' traffic, law enforcement agencies need the surveillance information to be logically, physically, or otherwise separated and protected from access by the carrier's subscribers.

TCs are not expected to ensure a level of security for intercept access and transparency beyond the capabilities of their own equipment.

3.4.2.2. *Encryption of Delivered Communication-Identifying Information and Communication Content*

The confidentiality and transparency of surveillance data must be protected as it transits between the TC delivery function and the LEA monitoring facility.

(EC) 39. If shared network resources are to be used for the delivery of communication-*identifying information* and *communication* content to an *LEA*, law enforcement needs the communication-identifying information and communication content to be encrypted on the delivery interface.

3.4.3. Procedural Safeguards

TCs are expected to institute prudent procedures and apply technical solutions, where necessary, to maintain the confidentiality and transparency of intercepted communications. Such measures should be consistent with the risk of compromising the information pertaining to intercept activities.

(EC) 40. Law enforcement agencies need TCs to establish operating practices and procedures containing safeguards that preclude unauthorized or improper access to or use of interception capabilities and to prevent any compromises of transparency.

Examples of such procedural safeguards include:

- a. Restrictions on access to information about interception capabilities;
- b. Physical security to limit access to systems controlling or supporting interceptions;
- c. Security mechanisms for activating and deactivating interceptions or accessing captured communication-identifying information or communications content (e.g., via access passwords and possibly case-level security);
- d. Procedures to prevent subjects from being notified of service changes caused by the implementation of interceptions;
- e. Restriction of knowledge of interceptions to authorized telecommunications carrier personnel (i.e., personnel with a “need-to-know”).

3.5. Capacity and Transmission Bandwidth

3.5.1. Simultaneous Interceptions

(EC) 41. Law enforcement agencies must be able to perform multiple, simultaneous interceptions within a carrier’s network and at each of its relevant network elements (Intercept Access Points) located throughout the carrier’s service area. The capability for multiple, simultaneous interceptions shall include the following:

1. Ability to access and monitor all simultaneous communications originated, received, or redirected by the intercept subject.
2. Ability for multiple law enforcement agencies to monitor, simultaneously, the same intercept subject while maintaining transparency, including between agencies. Up to five LEAs must be able to simultaneously monitor the same intercept subject.
3. Ability of the TCs to simultaneously support a number of separate (i.e., multiple subjects) legally authorized interceptions within its service area, including different levels of authorization for each interception (i.e., communication-identifying information only, or communication-identifying information and communication content).

1

2 **3.5.2. *Transmission Bandwidth***

3

4 Individual law enforcement agencies are responsible, with the assistance of carriers, for ordering and
5 acquiring sufficient transmission bandwidth from each TC in a timely manner for the lawful
6 interception capability to be performed and for communication-identifying information and
7 communication content to be delivered from the TC to the LEA's collection system(s) such that the
8 required number of intercept subjects and their packet-based service characteristics can be
9 appropriately handled.

10

11 **4. Recommendation**

12

13 It is proposed that this Stage 1 description be incorporated into Section 4 (Stage 1 Description: User
14 Perspective) of J-STD-025, Revision B. The J-STD-025 specification's Stage 1 description only
15 minimally addresses surveillance capabilities for packet-based communications (i.e., Section 4.6.3,
16 Packet Data IAP), where full content is being provided for selected packet streams. It is proposed that
17 the Stage 1 material from this contribution be incorporated within Section 4. The detailed
18 organization of the section structure and any needed revisions to existing text for circuit-mode
19 surveillance are for further study.

20

APPENDIX B

TIBALLOT

From: Les Szwajkowski [lmski@fbi.gov]
Sent: Wednesday, September 17, 2003 2:38 PM
To: TIBALLOT
Cc: pdhollar@lafayettegroup.com
Subject: T I Letter Ballot LB 1174

ACCREDITED STANDARDS COMMITTEE
T I-TELECOMMUNICATIONS
LETTER BALLOT

**** -ACTION REQUESTED -****

REPLY TO: ATIS Letter Ballot Number: LB 1174
T I Secretariat Document Number: J-STD-025B
1200 G St., NW, Suite 500 Date: 08/19/03
Washington, DC 20005 Ballot Period: 4 Weeks
FAX: 202.347.7125 Ballot Closes: 09/17/03
EM: tibalbot@atis.org

Authorized By: T1P1/T1S1
Distributed By: T I Secretariat

Subject: Draft Proposed Trial-Use/Interim Standard - Lawfully
Authorized Electronic Surveillance (Joint TIA/T1
draft proposal)

Statement: The T1P1 and T1S1 members at their August 2003
plenary approved this draft proposed
Trial-Use/Interim Standard for letter ballot. This
draft ANSI for Trial-Use is under the Joint T1/TIA
Standards Document (JSD) Process where TIA is the
lead organization and sole submitter to ANSI.
Please note: Due to an interest category imbalance
at the time of this letter ballot, weighted voting
of a .87 value applies to the manufacturing interest
group.

Question: Do you approve this draft proposed standard for
Trial-Use per ANSI procedures for future submittal
to ANSI for approval as an American National
Standard?

Ballot: YES _____ NO X (Comments Required)

Ballot: YES _____ (w/ comments) ABSTAIN _____ (w/ reasons)

ABSTAIN _____

(IF VOTING "NO, WILL VOTE CHANGE TO "YES" IF THE ATTACHED
CHANGES ARE MADE?)

YES X NO _____

Signature –Leslie M. Szwajkowski_____ Principal_X_ Alternate_____

Organization _FBI-CIU (formally the ESTS)_____ DATE_9/17/03

Telephone #. –703-814-4808_____

ESTS's comments are attached

LB 1174

Vote:

The CALEA Implementation Unit (CIU) (formerly the Electronic Surveillance Technology Section) of the Federal Bureau of Investigation has reviewed Letter Ballot 1174 (LB 1174) (PN-4465-RV1) and has concluded that the document does not supply Law Enforcement (LE) with the capabilities it needs to perform surveillance activities for packet-mode communications. CIU has also concluded that LB 1174 does not provide the level of detail necessary for a document of this importance and is likely to create confusion for Telecommunication Service Providers (TSPs), equipment manufacturers, and LE in their efforts to implement packet-mode surveillance. As a result of both the deficiencies and the insufficient level of detail in the proposed J-STD-025-B (as discussed below) CIU votes **No** on LB 1174 and maintains that J-STD-025-B should not be adopted as the standard for packet-mode communications.

General Comments:

The stated intent of J-STD-025-B is to define "...the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance." CIU's position is that the revised document J-STD-025-B is significantly deficient in addressing packet-mode communications. Therefore, CIU cannot support adoption of a deficient standard that will have the effect of affording TSPs or equipment manufacturers "safe harbor" with respect to packet-mode communications.

LE is the sole user of the surveillance capabilities described in the document. Notwithstanding this, CIU believes that the expressed needs of LE with regard to packet-mode communications were given only cursory consideration during the development of J-STD-025-B. LE, through CIU, expended considerable effort throughout the course of the J-STD-025-B developmental timeline to (1) propose an approach to packet-mode surveillance that would best meet the needs of LE while minimizing the cost of development and implementation and (2) develop the Stage 1 language and requirements for packet-mode surveillance in a technology-neutral manner. The following list of CIU's contributions clearly demonstrates the extent of LE's efforts to convey its needs to TR45 LAES Ad Hoc Group:

- TR45.LAES/2001.08.29: Proposal for work product of TR 45 LAES Ad Hoc Group work on Packet-Mode Data Surveillance Capabilities to be contained in a new document.
- TR45.LAES/2001.11.07.06: Overview of Packet Surveillance Fundamental Needs for Law Enforcement.
- TR45.LAES/2001.12.18.02: Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.01.21.06: Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.01.21.03: Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities for packet-based communications pursuant to the Communications Assistance for Law Enforcement Act (CALEA).
- TR45.LAES/2002.02.12.05 (plus Revision 1): Framework for Development of LAES of Packet-based Communications.

- TR45.LAES/2002.02.12.09: Comments on Motorola Contribution (TR LAES/2002.02.12.03) on CALEA Requirements and Quotations.
- TR45.LAES/2002.04.22.03 (plus Revision 1): Stage 1 material for PN-4465-RV1.
- TR45.LAES/2002.05.21.03: Stage 1 material for PN-4465-RV1.

In particular, contribution TR45.LAES/2002.01.21.06 provided a comprehensive Stage 1 description of LE's needs including 41 essential capabilities specifically worded to cover the differences in terminology and technology between packet-mode and circuit-mode communications. This contribution and others made by CIU were repeatedly rejected based on the argument that the definitions or requirements were "already in the document." CIU made these contributions principally because, in its view, the existing standard (J-STD-025A) makes explicit reference to circuit-mode technology but not packet-mode technology and, therefore, the new language was critical to the stated goal of creating the expanded standard

The net effect of the TR45 LAES Ad Hoc Group's consistent rejection of the contributions submitted by CIU relevant to LE's needs as sole user of the capability is to render the J-STD-025-B document essentially equivalent to the existing J-STD-025-A document. For example, J-STD-025-B contains no detailed requirements for services such as voice over packet communications. The J-STD-025-B document, in its present form, is, therefore, superfluous and of no value to either the industry or LE.

More specifically, CIU finds that J-STD-025-B, as circulated for balloting, is deficient in the following areas which are of major concern to LE:

1. Terminology does not include the concept of a 'session' as distinct from a 'call.'
2. Subject and associate's media information (e.g., network address, media format) would not be reported.
3. Bandwidth and bearer control events associated with the call would not be reported
4. Intercept subject and associate's contact address information would not be reported (if these become available during, for example, SIP-based call setup).
5. Definitions for party identities have not been extended to support identifiers used by common packet protocols (e.g., URI for SIP).
6. Concept of reporting location (of a mobile subscriber) would not include personal mobility (e.g., common for SIP phones).
7. Address registration and de-registration would not be reported
8. Reporting of post-cut-through addresses would not be extended to addresses other than E.164 numbers (e.g., a SIP URI).
9. Intercept subject's request for permission to originate or terminate a call to/from an associate would not be reported (needed for cases where the call control signaling would not be reported because call control is end-to-end and therefore not performed by the carrier's call management nodes).
10. Address resolutions would not be reported
11. Certain call redirections would not be reported, even when the subject's service is aware of them (e.g., associate redirections occurring subsequent to the subject becoming involved in a call).
12. Call release information (e.g., cause) known/used by the subject's service would not be reported.
13. Regarding cdma2000 intercept solution, the rejection of TR45.LAES/2002.01.21.06 containing the Stage 1 language and requirements by TR45 LAES Ad Hoc Group for

the “common” requirements sections of the standard render the technology-specific cdma2000 interception solution deficient. Critical topics such as performance, reliability, security, and capacity, specific to packet-mode *communications*, are missing.

14. Packet Activity Reporting (i.e., reporting of IP address and transport layer port number information for the source and destination of an IP packet) is vital to any packet data surveillance solution and is missing from the cdma2000 interception solution.
15. For cdma2000, the location information that can be provided at the beginning and end of a session is limited to cell site identification. Technology has already been developed that can provide more accurate location information such as longitude and latitude, and this should be reported to LE when available in the network.

While some might argue that the detailed requirements for packet-mode communications are found in normative references listed within J-STD-025B, CIU and LE are being asked to approve a standard that would be afforded “safe harbor” status for packet-mode surveillance that:

1. does not reflect LE’s stated User requirements
2. does not contain the text of specific requirements for enabling surveillance of packet-mode communications and
3. cites, as a normative reference for packet-mode surveillance capabilities, a document that is incomplete and furthermore does not have “safe harbor” status itself.

In light of the above, CIU’s position is that J-STD-025B, in and of itself, lacks specific requirements for packet-mode communications and, therefore, cannot be claimed to have “safe harbor” status for packet-mode communications.

For these reasons, CIU believes J-STD-025B should not be adopted, and that TSPs and equipment manufacturers should not be afforded “safe-harbor” with respect to packet-mode communications by virtue of their compliance with a deficient standard (J-STD-025-B).

APPENDIX C



U.S. Department of Justice

Federal Bureau of Investigation

*Electronic Surveillance Technology Section
14800 Conference Center Drive, Suite 300
Chantilly, VA 20151*

April 16, 2004

Re: Reply to "Call for Comments" on J-STD-025-B as a Trial Use Standard

Ms. Susan Carioti
ATIS
1200 G St, NW, Suite 500
Washington, DC 20005

Dear Ms. Carioti:

This letter provides a reply to the call for comments on the use of J-STD-025-B as a Trial Use Standard announced in the March 19, 2004 issue of *ANSI Standards Action* as well as an explanation of the perceived futility of further interactions in the balloting process for this document, as TI has yielded all comment resolution procedures to TIA, where LE is not being treated fairly.

The fact that the CALEA Implementation Unit (CIU) of the FBI is dissatisfied with the content of proposed J-STD-025-B and the procedures followed to create it has not been a secret for some time. To wit, the following is a quote from a letter dated February 28, 2003, that was sent from the Electronic Surveillance Technology Section (ESTS), of which CIU is a part, to the Chairperson of the TIA TR 45 LAES AHG.

Attached to this letter is the set of comments that indicates the numerous technical issues

The undefined scope and approach **adopted** by the **group** has fostered the development of a work product **that is** ill defined and unusable. ESTS **submitted several** contributions **proposing a general approach**, and capabilities required by law enforcement for interception **of packet-based** communications, and none of these contributions were **accepted**. Further, the group has **broadened** its **scope** to include legal and **regulatory** issues well beyond the purview of any industry standards-setting organization. **This** has shifted the focus away from the development of technical interception capabilities.

Law Enforcement has with this proposed trial use standard and which was provided in this organization's response to the ballot of J-STD-025-B. As indicated in the official response to ESTS from TIA, which acted as the lead SDO in this joint activity with ATIS, no action was taken on these comments. "Due to the lack of a contribution or representation for CIU at the October meeting, discussion resulted in no further action being taken on the CIU ballot comments. No changes were made to PN-4465-RV1 as a result of your ballot comments. The overall status of your ballot comments is No Action'." While we have difficulty understanding how such an approach to comments on a proposed standard is consistent with that of an ANSI-accredited standards development organization, it is characteristic of the lack of serious consideration of the input by this organization. One may see extensive evidence of this by referencing the meeting reports of the TIA

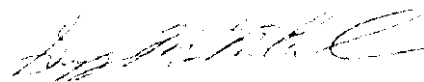
Ms. Susan Carioti
April 16, 2004

TR 45 LAES AHG - where this document was developed - for the record of how the contributions from Law Enforcement were treated.

It is important to observe that 47 USC § 1006(a)(1) specifically directs the Attorney General, in coordination with federal, state, and local Law Enforcement agencies to consult with appropriate associations and standards-setting organizations. The Attorney General has delegated its consultative authority under 47 USC § 1006(a)(1) to the Director of the Federal Bureau of Investigation, see 28 C.F.R. 0.85(o), which in turn tasked CIU with performing this required consultation. Therefore, CIU is representative of not just the FBI but of all Law Enforcement relative to consultation with industry in the matter of lawfully authorized electronic surveillance capability development. This clearly identifies this organization as an affected party and the sole voice for this constituency in the preparation of this proposed trial use (or "interim" in the parlance of TIA) standard. We note that the synopsis of the document in the *ANSI Standards Action* indicates that "this document defines the interfaces between a telecommunications service provider (TSP) and a law enforcement agency (LEA) to assist the LEA" Since ESTS is the official representative of one side of this interface standard and this organization believes that its input to the specification of this interface has been systematically and inappropriately discounted and ignored, it is hard to imagine a reasonable individual supporting that J-STD-025-B should be recognized as a trial use standard.

Furthermore, the lead SDO for this document continues to confuse the application of this document. In the same issue of *ANSI Standards Action* that J-STD-025-B is proposed as a trial use standard through January 1, 2007, TIA has announced a PINS to issue the document as an American National Standard. The project form approved by TIA TR 45 indicates a proposed completion date of June, 2004. As if this didn't cause enough confusion for the industry, the March 26 issue of *ANSI Standards Action* announced a PINS for J-STD-025-C - an extension of version B. The project form, approved by TIA TR 45, indicates a proposed completion date of November, 2004 for that document. Other correspondence will respond directly to the confusion introduced by these other documents.

Sincerely,



Greg Milonovich,

Supervisory Special Agent, FBI
CALEA Implementation Unit
(703) 814-4713

copy to:
Ms. Aivelis Colon, ATIS
Ms. Susan Hoyler, TIA
ANSI Board of Standards Review

Annex 1 - LB 1174 Vote by CIU

The CALEA Implementation Unit (CIU) of the Electronic Surveillance Technology Section of the Federal Bureau of Investigation has reviewed Letter Ballot 1174 (LB 1174) (PN-4465-RV1) and has concluded that the document **does not supply Law Enforcement (LE) with the capabilities it needs to perform** surveillance activities for packet-mode communications. *CIU has* also concluded that LB 1174 does not provide the level of detail necessary for a document **of** this importance and is likely to create confusion for Telecommunication Service Providers (TSPs), equipment manufacturers, and LE in their efforts to implement packet-mode surveillance. As a result of both the deficiencies and the insufficient level of detail in the proposed J-STD-025-B (as discussed below) CIU votes **No** on LB 1174 and maintains that J-STD-025-B should not be adopted as the standard for packet-mode communications.

General Comments:

The stated intent of J-STD-025-B is to define "...the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance." CIU's position is that the revised document J-STD-025-B is significantly deficient in addressing packet-mode communications. Therefore, CIU cannot support adoption of a deficient standard that will have the effect of affording TSPs or equipment manufacturers "safe harbor" with respect to packet-mode communications.

LE is the sole user of the surveillance capabilities described in the document

Notwithstanding this, CIU believes that the expressed needs of LE with regard to packet-mode communications were given only cursory consideration during the development of J-STD-025-B. LE, through CIU, expended considerable effort throughout the course of the J-STD-025-B developmental timeline to (1) propose an approach **to** packet-mode surveillance that would best meet the needs of LE while minimizing the cost of development and implementation and (2) develop the Stage 1 language and requirements for packet-mode surveillance in a technology-neutral manner. The following list of CIU's contributions clearly demonstrates the extent of **LE's** efforts to convey its needs to TR45 LAES Ad Hoc Group:

- TR45.LAES/2001.08.29: Proposal for work product of TR 45 LAES Ad Hoc Group work on Packet-Mode Data Surveillance Capabilities to be contained in a new document.
- TR45.LAES/2001.11.07.06: Overview of Packet Surveillance Fundamental Needs for Law Enforcement.
- TR45.LAES/2001.12.18.02: Framework for Development of LAES of Packetbased Communications.
- TR45.LAES/2002.01.21.06: Framework for Development of LAES of Packetbased Communications.
- TR45.LAES/2002.01.21.03: Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities for packet-based communications pursuant to the Communications Assistance for Law Enforcement Act (CALEA).
- TR45.LAES/2002.02.12.05 (plus Revision 1): Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.02.12.09: Comments on Motorola Contribution (TR LAES/2002.02.12.03) on CALEA Requirements and Quotations.
- TR45.LAES/2002.04.22.03 (plus Revision 1): Stage 1 material for PN-4465-RV1.
- TR45.LAES/2002.05.21.03: Stage 1 material for PN-4465-RV1.

In particular, contribution TR45.LAES/2002.01.21.06 provided a comprehensive Stage 1 description of LE's needs including 41 essential Capabilities specifically worded to cover the differences in terminology and technology between packet-mode and circuit-mode communications.

This contribution and others made by CIU were repeatedly rejected based on the argument that the definitions or requirements were "already in the document." CIU made these contributions **principally because, in its view, the existing standard (J-STD-025A) makes explicit reference to** circuit-mode technology but not packet-mode technology and, therefore, the new language was critical to the stated goal of creating the expanded standard.

The net effect of the TR45 LAES Ad Hoc Group's consistent rejection of the contributions submitted by CIU relevant to LE's needs as sole user of the capability is to render the J-STD-025-B document essentially equivalent to the existing J-STD-025-A document. For example, J-STD-025-B contains no detailed requirements for services such as voice over packet communications.

The J-STD-025-B document, in its present form, is, therefore, superfluous and of no value to either the industry or LE.

More specifically, CIU finds that J-STD-025-B, as circulated for balloting, is deficient in the following areas which are of major concern to LE:

1. Terminology does not include the concept of a 'session' as distinct from a 'call.'
2. Subject and associate's media information (e.g., network address, media format) would not be reported.
3. Bandwidth and bearer control events associated with the call would not be reported
4. Intercept subject and associate's contact address information would not be reported (if these become available during, for example, SIP-based call setup).
5. Definitions for party identities have not been extended to support identifiers used by common packet protocols (e.g., URI for **SIP**).
6. Concept of reporting location (of a mobile subscriber) would not include personal mobility (e.g., common for SIP phones).
7. Address registration and de-registration would not be reported.
8. Reporting of post-cut-through addresses would not be extended to addresses other than E.164 numbers (e.g., a SIP URI).
9. Intercept subject's request for permission to originate or terminate a call to/from an associate would not be reported (needed for cases where the call control signaling would not be reported because call control is end-to-end and therefore not performed by the carrier's call management nodes).
10. Address resolutions would not be reported.
11. Certain call redirections would not be reported, even when **the** subject's service is aware of them (e.g., associate redirections occurring subsequent to the subject becoming involved in a call).
12. Call release information (e.g., cause) known/used by the subject's service would not be reported.
13. Regarding cdma2000 intercept solution, the rejection of **TR45.LAES/2002.01.21.06** containing the Stage 1 language and requirements by TR45 LAES Ad Hoc Group for the "common" requirements sections of the standard render the technology-specific cdma2000 interception solution deficient. Critical topics such as performance, reliability, security, and capacity, specific to packet-mode communications, are missing.
14. Packet Activity Reporting (i.e., reporting of IP address and transport layer port number information for the source and destination of an IP packet) is vital to any packet data surveillance solution and is missing from the cdma2000 interception solution.
15. For cdma2000, the location information that can be provided at the beginning and end of a session is limited to cell site identification. Technology has already been developed that can provide more accurate location information such as longitude and latitude, and this should

be reported to LE when available in the network.

While some might argue *that* the detailed requirements for packet-mode communications are found in normative references listed within J-STD-025B, CIU and LE are being asked to approve a standard that would be afforded "safe harbor" status for packet-mode surveillance that:

1. does not reflect LE's stated User requirements
2. does not contain the text of specific requirements for enabling surveillance of packet-mode communications and
3. cites, as **a** normative reference for packet-mode surveillance capabilities, a document that is incomplete and furthermore does not have "safe harbor" status itself.

In light of the above, CIU's position is that J-STD-025B, in and of itself, lacks specific requirements for packet-mode communications and, therefore, cannot be claimed to have "safe harbor" status for packet-mode communications.

For these reasons, CIU believes J-STD-025B should not be adopted, and that TSPs and equipment manufacturers should not be afforded "safe-harbor" with respect to packet-mode communications by virtue of their compliance with a deficient standard (J-STD-025B).